(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 December 2001 (27.12.2001)

PCT

(10) International Publication Number
WO 01/99379 A1

(51) International Patent Classification⁷: H04L 29/06

(21) International Application Number: PCT/GB00/04952

(22) International Filing Date:
21 December 2000 (21.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

0014980.7	19 June 2000 (19.06.2000)	GB
0023813.9	28 September 2000 (28.09.2000)	GB
0028109.7	17 November 2000 (17.11.2000)	GB

(71) Applicant and
(72) Inventor: GILBERT, Martin [GB/GB]; 41 St, Michaels, Longstanton, Cambridge CB4 5BZ (GB).

(74) Agent: REES, Alexander, Ellison; Urquhart-Dykes & Lord, 30 Welbeck Street, London W1G 8ER (GB).

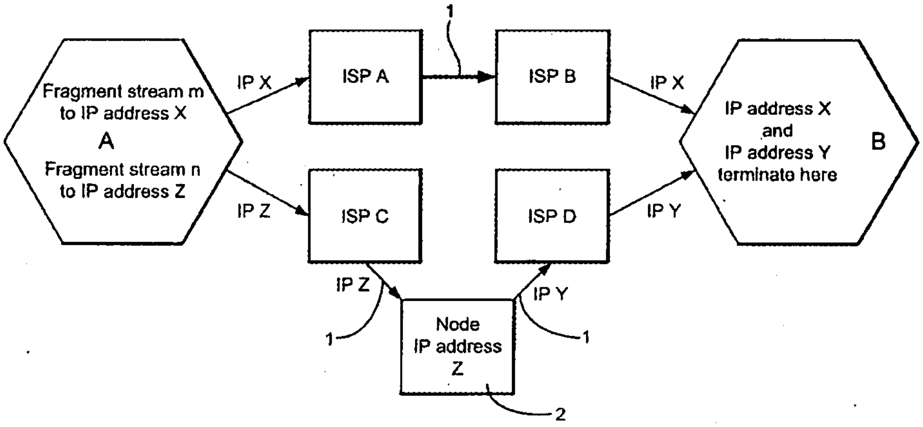
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE COMMUNICATIONS METHOD


1
Fragment stream m to IP address X
A
Fragment stream n to IP address Z
IP X
IP Z
ISP A
ISP B
ISP C
ISP D
IP X
IP Y
IP address X and IP address Y terminate here
B
IP Z
IP Y
Node IP address Z
1
1
2

(57) Abstract: A secure communications method comprises the steps of: fragmenting a digital message into a series of fragments shorter than the smallest base unit of data used by a communications network; dividing the fragments into a plurality of fragment streams; forming a plurality of partial messages, each incorporating a fragment stream; sending the plurality of partial messages through at least one digital communication network; and recombining the fragment streams from the partial messages to reproduce the digital message.

WO 01/99379 A1

Secure Communications Method

This invention relates to a secure communications method and particularly to a secure communications method for communication across a digital communications network.

Where a message is transmitted electronically across a digital communications network it is well known that there is a potential danger that the message may be intercepted by unauthorised third parties.

Traditionally, this problem has been addressed by the message originator encrypting the message before sending it. The authorised recipient of the message knows how to decrypt the message, so the message is still readily accessible to the intended recipient. However, unauthorised third parties do not know how to decrypt the message and so cannot gain access to the message even if they successfully intercept the encrypted message.

In practice however it is possible that the unauthorised third party may be able to decrypt the encrypted message and so gain unauthorised access to the message contents.

It is generally accepted that any encryption technique can be defeated if sufficient resources and time are spent on breaking the encryption to allow the original message to be read. As a result, the usual standard used in assessing the security of encrypted messages is to encrypt the message using an encryption technique which will take an unauthorised eavesdropper so much cost or time to decrypt that the original message will either not be of sufficient interest or value to justify the cost or will no longer be of interest or value by the time it is accessible.

Accordingly, the security of all messages sent over communications networks must be regarded as questionable, particularly because estimates of the time taken to break encryption must always be based on assumptions as to the resources and techniques available to the would be unauthorised third party attempting decryption.

A further problem is that the third party may have unauthorised access to the information required to decrypt the encrypted message so that the third party may be able to derive the original message from an intercepted encrypted message as quickly and easily as the intended recipient.

This invention is intended to provide a secure communications method overcoming these problems, at least in part.

This invention provides a secure communications method comprising the steps of:

fragmenting a digital message into a series of fragments;

dividing the fragments into a plurality of fragment streams;

forming a plurality of partial messages , each incorporating a fragment stream;

sending the plurality of partial messages through at least one digital communication network; and

recombining the fragment streams from the partial messages to reproduce the digital message, the length of the fragments being shorter than the smallest base unit of data used by the communications network.

This provides the advantage that a third party intercepting one of the partial messages cannot reproduce the overall message.

Advantageously, in order to make it more difficult for a third party to intercept all of the partial messages or to identify intercepted partial messages as relating to the same original message the partial messages may be sent to two or more network addresses.

Advantageously, some of the plurality of partial messages may be sent through different ones of two or more service providers and most preferably at least some of the plurality of partial messages may be sent through different ones of at least two separate networks.

Preferably, at least one of the partial messages is sent through an intermediate node.

Preferred embodiments of the invention will now be described by way of example only with reference to the accompanying diagrammatic figures, in which:

Figure 1 shows a first embodiment of the invention;

Figure 2 shows a second embodiment of the invention;

Figure 3 shows a third embodiment of the invention;

Figure 4 shows a fourth embodiment of the invention;

Figure 5 shows an example of the invention combining the third and fourth embodiments;

Figure 6 shows a fifth embodiment of the invention;

Figure 7 shows an example of the invention combining the fifth and third embodiments; and

Figure 8 shows a further example of the invention combining the third and fifth embodiments.

This invention is based on a realisation that the underlying reason why any encrypted message can be decrypted is that all of the information making up the original message is contained within the encrypted message. Accordingly, it is always theoretically possible for this information to be extracted from the encrypted message and the original message reproduced.

The basic concept of the invention is that a message to be sent from a message originator to a message recipient should be divided into multiple parts. These parts are then assembled to form multiple separate partial messages each containing only a part of original message information which are sent from the message originator to the message recipient.

The message recipient can recombine the information content of the multiple received partial messages to reproduce the original message. However, an unauthorised third party eavesdropper intercepting only some of the partial messages cannot reproduce the original message regardless of the resources or time spent in the attempt because the intercepted partial message or messages do not include all of the information content of the original message or allow the whole information content to be deduced, so that the information content of the original message cannot be extracted from the partial message. Further, if the parts into which the original message is divided are small relative to the size of the original message it will not even be possible to reproduce a part of the original message because without the missing parts of the original message the relationships between the parts of the original message contained in the intercepted partial message or messages cannot be determined or deduced.

In this application the term message is used. The term message is used only to refer to a quantity of digital information to be sent from an originator to a receiver. There is no requirement that the message be all of the information to be sent. A single communication session may involve the transfer of many messages. This digital information may represent numerical data or text but could also be image data or audio or video data.

The information making up the message may be encrypted by some known encryption technique before or after being broken into multiple parts or both. Such encryption can be added to the method of the present invention to increase the level of security provided but the use of such further encryption is optional and not essential.

In general, the greater the number of parts the original message is divided into and the greater the corresponding number of partial messages sent, the greater the degree of security provided. Further, the greater the degree of diversity in the routes by which the partial messages are sent from the originator to the receiver the greater the degree of security which will be provided as will be explained below.

An example of use of a first embodiment of the invention will now be described with reference to Figure 1.

In Figure 1 a message originator A wishes to send a message to a message recipient B.

The message is in the form of digital information and is divided up by A into a series of small fragments, each of which is smaller than the base unit of data normally used for communications. For example, computers typically use 8, 16 or 32 bit (binary digit) data units, to represent, store and transmit information.

The fragments may be in portions as small as one bit but more typically would be in the range 2 to 7 bits so that they were smaller than the smallest standard 8 bit data unit used. The series of fragments is then divided into two partial messages M and N each of which comprises a fragment stream m or fragment stream n.

The simplest approach is to divide the stream of fragments into partial messages by assigning fragments alternately or cyclically to partial messages, but more complex assignment methods may be used in order to make combination of partial messages to obtain the original message more difficult. Further, the order of the fragments in the partial messages may be altered.

In this example the message originator A and the message recipient B are able to communicate over the Internet 1 through respective first and second Internet service providers ISP A and ISP B.

The message originator A sends the partial messages M and N to the IP address X of the message recipient B by sending the two partial messages M and N to the first ISP A. The first ISP A then forwards the two partial messages M and N to the second ISP B through the Internet 1 and the second ISP B then sends the two partial messages M and N to message recipient B.

The message recipient B then recombines the fragment streams contained in the two partial messages M and N to reform the original message.

This method of the first embodiment is referred to as stream diversity because the partial messages are formed by separated streams of message fragments.

The partial messages M and N form separate logical groups of message fragments with no intrinsic coherence or other relationship between them except that they are destined for the same recipient. Only the message originator A and the message recipient B know the necessary relationship between the partial messages or the fragment streams which will allow the original message to be correctly reconstructed from the partial messages.

In the first embodiment the original message is only divided into two fragment streams and two corresponding partial messages. Any number of fragment streams and partial messages could be used, although in practice it is expected that the number of partial messages will normally be in the range 2 to 16.

In this embodiment, if an unauthorised third party intercepts one of the two partial messages they will not be able to reassemble the original message or any coherent part of the original message.

Further, even if a third party manages to intercept both of the partial messages they will not know how the information fragments contained in the two partial messages should be recombined to reproduce the original message.

Where the fragments are divided into more than two streams so that more than two partial messages are produced and sent, a third party will not be able to reassemble the original message even if several of the partial messages are intercepted, provided that not all of the partial messages are intercepted.

Although stream diversity as used in the first embodiment where the multiple partial messages are sent from the message originator A to the message recipient B through a single Internet route provides a level of security, this arrangement is vulnerable to a third party intercepting all of the partial messages because they are all transmitted along a single Internet route and so may pass along a single physical communications link. Although, as explained above, the third party will not know how to recombine the message fragments to reproduce the original message, a third party having all of the partial messages will have all of the information making up the original message, which is contained in the partial messages. Accordingly, similarly to a conventional encrypted message, it is theoretically possible for the original message to be reproduced from the partial messages.

In order to provide an increased level of security path diversity, in which the partial messages are sent along different communications links or routes can be used instead of the stream diversity of the first embodiment.

A second embodiment of the invention employing path diversity is shown in Figure 2.

In the second embodiment a message originator A wishes to send a message to a message recipient B and the message originator A and the message recipient B are able to communication over the Internet 1 through respective first and second Internet service providers ISP A and ISP B similarly to the first embodiment.

In the second embodiment the message originator A divides the original message into two fragment streams m and n as before. The fragment stream m is then sent as a first partial message M to an IP address X while the second fragment stream n is sent as a second partial message N to a second IP address Y. The two partial messages M and N are sent by the message originator A to the first ISP A. The first ISP A then sends the two partial messages through the Internet 1 to the second ISP B. The second ISP B then sends the first and second partial messages M and N to their respective destination IP addresses X and Y, both of which terminate at the message recipient B.

The message recipient B then recombines the two partial messages to reproduce the original message.

In the second embodiment the partial messages travel on a single Internet route and as a result, similarly to the first embodiment, they will commonly all be conveyed over the same network and path and the same physical communications link. However, in communication networks in which IP addresses are dynamically assigned during a single Internet access session this method will provide greater security because of the increased difficulty a third party will have in identifying the partial messages being sent to the two IP addresses X and Y as being partial messages carrying parts of the same original message and both being sent to the same message recipient B. Where IP addresses are static the technique of the second embodiment will provide little or no security advantage over the first embodiment.

In the described embodiment two partial messages are sent to the two corresponding IP addresses at the recipient B. Where the original message is split into more than two partial messages and these are sent to multiple IP addresses at the message recipient B the number of IP addresses may be less than the number of partial messages so that more than one partial message is sent to some or all of the multiple IP addresses.

In order to provide a greater degree of security and full path diversity indirect addressing of one of the partial messages can be used. That is, one of the partial messages can be sent directly from the message originator to the message recipient while another partial message is sent from the message originator to a remote node and then resent from the remote node to the message recipient.

A third embodiment of the invention employing indirect addressing to provide path diversity is shown in Figure 3.

Similarly to the second embodiment a message to be sent from a message originator A to a message recipient B through respective first and second Internet service providers ISP A and ISP B and the Internet 1, and the message recipient has two IP addresses X and Y.

As in the earlier embodiments the message originator A divides the original message into fragments to form it into two partial messages M and N. The message originator A addresses the first partial message M to go to the IP address X of the message recipient B while the second partial message N is addressed to go to an IP address Z associated with a node 2.

The node 2 is connected to the first and second ISP A and ISP B through the Internet 1 and it able to receive and resend messages.

The message originator A forwards the two partial messages M and N to the first ISP A and the first ISP A then sends the first partial message M through the Internet 1 to the second ISP B and sends the second partial message N through the Internet 1 to the address Z of the node 2.

The node 2 receives the second partial message N at its IP address Z and then resends the second partial message N to the IP address Y of the message recipient B by sending the second partial messages N through the Internet 1 to the second ISP B.

The second ISP B sends the first and second partial messages M and N to the IP addresses X and Y of the message recipient B. It should be noted that the times at which the ISP B sends the first and second partial messages M and N to the message recipient B are incoherent and have no specified relationship.

The full path diversity of the third embodiment makes interception and correlation of the partial messages by an unauthorised third party more difficult because the path followed by the first partial message from the first ISP A directly to the second ISP B is different from the path followed by the second partial message N from the first ISP A to the node 2 and then to the second ISP B and this different route will normally involve the first and second partial messages M and N travelling along different physical communications links. This route and physical separation of the partial messages M and N can be ensured by the use of a node 2 which is physically remote from the first and second ISP A and ISP B. Further, the second partial message N spends part of its journey addressed as a message travelling from the message originator A to the node 2 and another part of its journey addressed as a message from the node 2 to the message recipient B. As it result, it will be difficult for a third party to identify a second partial message N as being related to the first partial message M which is addressed directly from the message originator A to the message recipient B.

In the third embodiment the two partial messages M and N are sent to two different IP addresses X and Y at the message recipient B. This arrangement is preferred in order to provide the security advantages described with reference to the second embodiment, particularly in communication networks in which IP addresses are dynamically assigned during a single access session. However, the two partial messages M and N could both be sent to the same IP address of the message recipient B, although this would reduce the degree of security provided.

It should be noted that because communication networks rely on the address information carried by a message to deliver the message to the correct recipient it is not possible to disguise the fact that the first partial message M is being sent to an IP address of the message recipient B. However, while the second partial message is travelling between the message originator A and the node 2 the network only requires that the IP address of the node 2 be identified and accordingly the ultimate destination at the message recipient B can be concealed. This could be carried out by not including the ultimate IP address of the message recipient B in the second partial message M at all but instead instructing the node 2 to always forward messages received at its IP address instead to the IP address Y of the message recipient B. Alternatively, the destination IP address at the message recipient B could be concealed by encryption or by the second partial message N, or at least the part of it identifying the final destination address at the message recipient B, itself being divided into two or more partial messages so that these partial messages must be recombined at the node 2 in order to allow the ultimate destination to be identified.

Further, multiple nodes 2 could be arranged in series so that a partial message passes from one node to another node. Also, the partial message routes could be selected so that all of the partial messages pass through at least one node 2. Use of multiple nodes in this way will allow the true recipient or originator of the original message to be completely concealed from eavesdroppers.

In order to provide a greater degree of security, path diversity can be increased further by the use of multiple network connections. That is, if both the message originator A and the message recipient B are connected to the Internet through two separate ISP's the partial messages can be sent through different pairs of ISP's so that route and physical separation of the partial messages is assured even when the message is being handled by the ISP's themselves.

A fourth embodiment of the invention employing multiple connection to provide path diversity is shown in Figure 4. Similarly to the second embodiment, a message originator A is able to communicate with a message originator B through the Internet 1. In the fourth embodiment the message originator A has associated first and third Internet service providers ISP A and ISP C while second and fourth Internet service providers ISP B and ISP D are associated with the message recipient B.

As in the earlier embodiments the message originator A divides the original message into fragments to form it into two partial messages M and N. The message originator A addresses the first partial message M to go to the IP address X of the message recipient B while the second partial message N is addressed to go to a second IP address Y of the message recipient B.

The message originator A forwards the two partial messages M and N to the first ISP A and third ISP C respectively. The first ISP A then sends the first partial message M through the Internet 1 to the second ISP B while the third ISP C sends the second partial message N through the Internet 1 to the fourth ISP D.

The second ISP B sends the first partial message M to the IP address X of the message recipient B while the fourth ISP D sends the second partial message N to the IP address Y of the message recipient B.

The first and third ISP A and ISP C and the second and four ISP B and ISP D will normally be physically remote from one another so that the communication path through the Internet 1 followed by the two partial messages and the physical communications links they traverse will be entirely different, making interception and correlation of the first and second partial messages by third parties difficult.

In the present application correlation of the partial messages is used to mean the correct identification of partial messages as being partial messages derived from the same original message.

In the fourth embodiment the two partial messages M and N are sent to different IP addresses X and Y of the message recipient B. For the reasons explained above regarding the second embodiment this arrangement is preferred to increase security. However, the two partial messages M and N could both be sent to the same IP address of the message recipient B provided that this IP address was accessible to both the second and fourth ISP B and ISP D, although this would reduce the degree of security provided.

In order to provide a still greater degree of security, path diversity can be increased still further by combining of the third and fourth embodiments. That is, in addition to the use of multiple connection through multiple ISP's, the path of one of the partial messages through the ISP's could be extended to pass through a proxy node.

Such an arrangement combining the features of the third and fourth embodiments is shown in Figure 5.

The arrangement of Figure 5 is based on the arrangement of Figure 4 and functions similarly except that a node 2 is provided connected to the third and fourth ISP C and ISP D.

Similarly to the fourth embodiment the message originator A divides the original message into fragments to form it into two partial messages M and N. The first partial message M is sent to the IP address X of the message recipient B by the message originator A forwarding it to the first ISP A. The first ISP A then sends the first partial message M through the Internet 1 to the second ISP B. The second ISP B then sends the first partial message M to the IP address X of the message recipient B.

The message originator A addresses the second partial message N to go to the IP address Z of the node 2 and forwards the second partial message N to the third ISP C. The third ISP C forwards the second partial message N through the Internet 1 to the IP address Z of the node 2.

The node 2 receives the second partial message N at its IP address Z and then resends the second partial message N to the IP address Y of the message recipient B by forwarding the second partial message N through the Internet 1 to the fourth ISP D. The fourth ISP D then sends the second partial message N to the IP address Y of the message recipient B.

The example of Figure 5 combining the third and fourth embodiments of the invention provides increased security against interception by providing full path diversity and also ensuring that the second partial message N spends part of its journey addressed as a message travelling from the message originator A to the node 2 and then a part of its journey addressed as a message from the node 2 to the message recipient B. As a result, not only will it be difficult for a third party to successfully intercept both of the partial messages because they are communicated along entirely different routes through different ISP's but it will also be difficult for the third party to identify the first and second partial messages M and N as being related to one another.

The combined arrangement of Figure 5 will also avoid problems in the unusual situation that two of the four ISP's are physically close together so that the separate communications routes in fact pass through the same physical communications links.

In order to obtain the best level of security network diversity can be used. That is, the first and second partial messages can be sent through separate communications networks.

A fifth embodiment of the invention employing network diversity is shown in Figure 6.

In the fifth embodiment the message originator A and the message recipient B are able to communicate through two separate networks, network 1 and network 3. In this case network 1 is the Internet 1 and network 3 is another network such as a satellite communications network 3.

The message originator A divides the message into two streams of fragments which are incorporated into first and second partial messages M and N in the same way as in the previous embodiments. The first partial message M is sent to an Internet IP address X at the message recipient B while the second partial message N is sent to a satellite network address Q at the message recipient B.

The message originator A sends the first partial message to the first ISP A. The first ISP A passes the message through the Internet 1 to the second ISP B. Finally, the second ISP B sends the first partial message to the IP address X of the message recipient B.

The message originator A sends the second partial message N to a first satellite network service provider NSP E. The first satellite NSP E sends the second partial message through the satellite network 3 to a second satellite NSP F. The second NSP F then sends the second partial message N to a network address Q of the message recipient B.

By the use of network diversity in the fifth embodiment the difficulty encountered by an unauthorised third party in intercepting both partial messages is further increased because the two partial message travel along different routes through different physical communications links forming parts of different networks.

In practice very few third parties will have the resources or capability to intercept messages travelling along two separate communications networks. Even if a third party is able to intercept messages travelling through two separate networks, network 1 and network 3 in the example, in principle, it will be extremely difficult for a third party to identify the two partial messages travelling through the first and second separate networks as both being from the message originator A to the message recipient B and being partial messages relating to the same original message.

The network diversity of the fifth embodiment can be combined with the use of proxy nodes according to the third embodiment.

An example of such a combination is shown in Figure 7 which is based on the fifth embodiment shown in Figure 6. In the example of Figure 7, a proxy node 4 is connected to the satellite network 3 for communication with the first NSP E and the second NSP F.

In the example of Figure 7 the first partial message M is sent by the message originator A to the message recipient B through the first ISP A, the second ISP B and the Internet 1 as in the fifth embodiment. The second partial message N is sent by the message originator A to a network address P of the node 4. The message originator A sends the second partial message N to the first NSP E which sends it to the network address P of the node 4 through the satellite network 3. The node 4 receives the second partial message N at the network address P and then resends the second partial message N to the network address Q of the message recipient B. The node 4 forwards a second partial message N to the second NSP F through the satellite network 3 and the second NSP F sends the second partial message N to the network address Q of the message recipient.

The message recipient B then recombines the message fragments in the first and second partial messages M and N to reproduce the original message.

The use of a node 4 increases the degree of security provided to a higher level than is provided by network diversity alone by making it more difficult for a third party to successfully intercept the partial messages and making it more difficult for a third party to correlate intercepted partial messages as being partial messages derived from the same original message.

In the examples above of the fourth and fifth embodiments of the invention employing multiple connection and network diversity respectively the message originator A and message recipient B are each connected to a network or networks by two service providers. If this is not possible and only one of the message originator A and message recipient B is connected to two service providers the invention is still applicable and can provide improved security, although not to as great a degree as when both the message originator A and the message recipient B are connected to two service providers.

An example of the invention showing such a situation where the message originator A is connected to two separate service provider serving separate networks but the message recipient B is only connected to a single service providers is shown in Figure 8.

The example of Figure 8 is based on the example of the fifth embodiment shown in Figure 6 and the example of Figure 7. In the example of Figure 8 the message recipient B is connected to a single service provider SPG connected to the Internet 1 and to the satellite network 3 for communication with the first ISP A and the node 4 respectively.

In the example of Figure 8 the message originator A divides the message into two streams of fragments which are incorporated into first and second partial messages M and N in the same way as in the previous embodiments and examples. The first partial message M is sent to an IP address X at the message recipient B while the second partial message is sent to a satellite network address Q also at the message recipient B.

The message originator A sends the first partial message to the first ISP A. The first ISP A passes the message through the Internet 1 to the service provider SP G. Finally, SP G sends the first partial message to the IP address X of the message recipient B.

The message originator A sends the second partial message N to a network address P of the node 4. The message originator A sends the second partial message N to the first NSP E which sends it to the network address P of the node 4 through the satellite network 3. The node 4 receives the second partial message N at the network address P and then resends the second partial message N to the network address Q of the message recipient B. The node 4 forwards the second partial message N to the service provider SP G through the satellite network 3. Finally, the SP G sends the second partial message N to the network address Q of the message recipient.

Then, the message recipient recombines the message fragments contained in the two partial messages to reproduce the original message.

It will be appreciated that the example of Figure 8 provides less security than the example of Figure 7 which is a corresponding arrangement in which B is connected to separate network service providers rather than a single service provider connected to both networks because both partial messages are routed through a single service provider SP G. However, because the two partial messages travel through separate networks for some of their journey between the message originator A and the message recipient B and one of the partial messages is routed through a proxy node 4, the example of Figure 8 will provide greater security than the use of stream and path diversity according to the first to third embodiments in which the message recipient B is also only connected to a single service provider.

It will be appreciated that the embodiments and examples described above are purely specific examples of the invention. The use of the Internet and IP addresses is described in the examples for simplicity because the Internet is expected to be the most commonly used network for the foreseeable future. However, it should be understood that the invention can be used in other types of network and that where this is done appropriate network addresses should be used in place of IP addresses. For example, instead of IP addresses ATM (asynchronous transfer mode) virtual circuits could be specified as addresses where appropriate. It should be appreciated that the network across which the partial messages are sent could be an internal network within a device. Further, the invention can be applied, where appropriate, to the physical layer or transport layer, rather than the network layer, as alternative applications, for example, by means of photon-switching between fibre optic cables, or between fibres within such a cable. Similarly, diverse communications could be established using different channels or transponders on a communications satellite, or different satellites. Where the Internet is used in the examples the use of Internet service providers (ISP's) is specified. If other networks are used appropriate network service providers would be employed.

In the illustrated examples the message originator and message recipient are shown as being distinct from the service providers. This will usually be the case but it would of course be possible for the message originator or message recipient to be a service provider. However, even where this is the case it will normally be possible to distinguish the functions of dividing an original message into fragments and partial messages and recombining the partial messages and fragments into the original message at the message originator and message recipient respectively from the service provider function.

In the described embodiments and examples the invention is discussed in terms of the original message being divided into two streams of fragments which are in turn incorporated into two partial messages. This is the simplest way of carrying out the invention but an original message could be divided into a larger number of fragment streams and sent as a corresponding number of partial messages. In practice it is expected that the number of fragment streams and corresponding number of partial messages will be in the range 2 to 16 is most applications.

The described embodiments can be combined to provide increased levels of security. In principle there is no limit to how complex the routing arrangements of the different partial messages between the message originator and a message recipient can be. Similarly to conventional encryption based security systems the limits in practical embodiments will be set by the increased cost of sending messages by very complex routes.

In general the described first to fifth embodiments provide increasing levels of security, but the methods of the earlier embodiments can be incorporated into the methods of the later embodiments. For instance, as shown in the example of Figure 7 the route diversity by the use of nodes of the third embodiment can be used together with the network diversity of the fifth embodiment. Multiple connection diversity according to the fourth embodiment can also be provided within an or each network when network diversity according to the fifth embodiment is used. These combinations both require that the number of partial messages was greater than the number of networks.

Similarly, where path or network diversity according to the third to fifth embodiments is used, stream diversity according to the first embodiment or path diversity according to the second embodiment could be provided by dividing the original message into a greater number of partial messages than the number of connections or networks so that multiple partial messages are passed along each of the separate networks or connection paths.

Similarly, where nodes are used the possible methods are not limited to the use of a single node to receive and resend a single partial message. It would be possible for one, some or all of the partial messages to be sent by routes employing nodes. Further, it would be possible for one node to readdress a received partial message and send it on to a further node, this being repeated as many times as desired before the partial message is finally sent to the message recipient.

In the above description and embodiments and examples the secure communications method according to the invention is described in terms of the sending of messages from a message originator to a message recipient. It will be understood that the communications method is fully reversible so that messages can similarly and simultaneously be sent from the message recipient to the message originator, even in the non-symmetrical example of Figure 8. Similarly, it will be understood that the method can be used by a message originator to send the same message to multiple message recipients.

When an original message is formed into a number of partial messages, the original message is broken into a series of message fragments. As explained above, the message fragments should be smaller than the base unit used for communication in the networks employed and will typically be in the range 2 to 7 bits. In theory the individual fragments could be sent as separate partial messages. However, this will result in a very large number of partial messages so that it will normally be preferred to include a plurality of message fragments within each partial message. The simplest method of arranging this is to separate the original message into fragments and then assign the fragments in turn to the plurality of partial messages, the assignment being carried out cyclically.

This method of assigning message fragments to partial messages will result in each of the partial messages contained approximately the same number of message fragments so that the partial messages will be of approximately equal size. This is not essential and the message fragments could be assigned to the partial messages to result in different partial messages containing different numbers of message fragments.

One possible use of the invention which the message fragments would be differentially assigned could be in sending video signals where only an occasional message fragment is extracted from the video data stream and the video signal is sent with most of the video data being in a first partial message with only the very much smaller amount of data carried by the separated fragments being sent as a second partial message. Although in this case the partial message containing the bulk of the video data would contain nearly all of the video data it will still not be possible to view and display the video without combining the two partial messages because the locations at which the missing fragments should be inserted would not be known.

As explained above, the simplest method of carrying out the invention is to divide the message fragments evenly between a plurality of partial messages so that the partial messages are all essentially the same size. However, when network diversity according to the fifth embodiment is used the cost of using different ones of the networks may be significantly different. For example, in the described embodiments and examples, it would normally be expected that the cost of sending data through a satellite communications network would be greater than the cost of sending data through the Internet. When this is the case, in order to minimise the cost of sending messages using the inventive method it may be convenient to assign more message fragments to the message to be sent through the cheaper network than to the partial message to be sent through the more expensive network. An alternative or complimentary approach would be to assign the message fragments from the original message to more than two partial messages and send only one of the partial messages through a more expensive network with all of the others being sent through the cheaper network.

In order to ensure that individual partial messages cannot allow the original message to be inferred or deduced, where the original message is very short, for example yes or no, it is preferred that the original message is bulked out with meaningless padding information to ensure that the fragmentation process effectively obscures the original message.

The embodiments and examples described relate to the use of separate networks in parallel in order to provide security enhancing network diversity. It would of course be possible for individual partial messages to travel through two or more separate networks in series. However, such transmission of partial messages through multiple networks in series will not provide the advantage of network diversity in its own right. However, it is expected that employing message routes for the partial messages passing through two or more networks in series will provide some security advantage by making it more difficult for a third party intercepting the partial messages to identify them as part of the messages travelling from the message originator to the message recipient. This is expected to be particularly advantageous in enhancing security if a node is used able to receive messages through one network and to retransmit them through another network.

Where a node is used, the possibility of sending two partial messages to the node from the message originator and the node recombining the two partial messages to provide a further partial message to be forwarded to the message recipient identifying the message recipient is discussed above with reference to the third embodiment of the invention only. It will be understood that such a technique of fragmenting partial messages to form second or higher generation partial messages and recombining the second or higher generation partial messages at intermediate nodes to reproduce the partial messages to be sent to the message recipient so that the address or identity of the message recipient cannot be deduced from the second or higher generation partial messages is equally applicable to the methods of the fourth and fifth embodiments and the examples.

It should be noted that the partial messages and the fragment streams incorporated into the partial messages are asynchronous. This is necessary in order to allow for the differences in transmission times through different networks or along different routes through the same network. Further, this asynchronicity provides the advantage that a third party eavesdropper cannot deduce that two partial messages simultaneously received at two addresses associated with the message recipient must be derived from the same original message. In view of this asynchronicity, it should be understood that references to the order in which the partial messages travel along separate routes or pass between the message originator and the message recipient should only be taken as indicating a defined temporal relationship where they refer to the same partial message and should not be taken as implying any defined temporal relationship between events relating to different partial messages. That is, in the described embodiments and examples each partial message must travel through the various stages of its journey in order but there is no defined temporal relationship between the times at which different stages are carried out by different ones of the partial messages.

The invention is applicable to any digital communications network, including electronic and optical networks. The examples described above relate to the use of the invention on the Internet using IP addresses. The invention is equally applicable for use with ATM where virtual circuits are used analogously to the IP addresses in the examples.

The embodiments and examples described herein as described by way of example only and the person skilled in the art will be able to see ways in which these could be combined and extended all remaining with the scope of the invention as defined by the appended claims.

Claims:

1. A secure communications method comprising the steps of:
fragmenting a digital message into a series of fragments;
dividing the fragments into a plurality of fragment streams;
forming a plurality of partial messages , each incorporating a fragment stream;
sending the plurality of partial messages through at least one digital communication network; and
recombining the fragment streams from the partial messages to reproduce the digital message, the length of the fragments being shorter than the smallest base unit of data used by the communications network.

2. A method according to claim 1 in which the plurality of partial messages are sent from a message originator to a message receiver, the message receiver has at least two network addresses and at least one of the plurality of partial messages is sent to each of the network addresses.

3. A method according to claim 1 or claim 2, in which the plurality of partial messages are sent from a message originator to a message receiver, at least one of the message originator and the message receiver is connected to at least two network service providers and at least one of the plurality of partial messages is sent through each service provider.

4. A method according to claim 3, in which the message originator and message receiver are both connected to at least two respective service providers and at least one of the plurality of partial messages is sent through each service provider.

5. A method according to any preceding claim, in which the plurality of partial messages are sent from a message originator to a message receiver, at least one of the message originator and the message receiver is connected to at least two

digital communications networks and at least one of the plurality of partial messages is sent through each network.

6. A method according to claim 5, in which the message originator and the message receiver are both connected to at least two digital communications networks and at least one of the plurality of partial messages is sent through each network.

7. A method according to any preceding claim, in which the plurality of partial messages are sent from a message originator to a message receiver and at least one of the plurality of partial messages is sent from the message originator to a node and then resent from the node to the message receiver.

8. A method according to any preceding claim in which the, or one digital communications network is the Internet.

9. A method according to claim 2 in which different numbers of partial messages are sent to different ones of the network addresses.

10. A method according to claim 3 or claim 4 in which different numbers of partial messages are sent through different ones of the service providers.

11. A method according to claim 5 or claim 6 in which different numbers of partial messages are sent through different ones of the networks.

12. Apparatus arranged to carry out the secure communications method of any preceding claim.

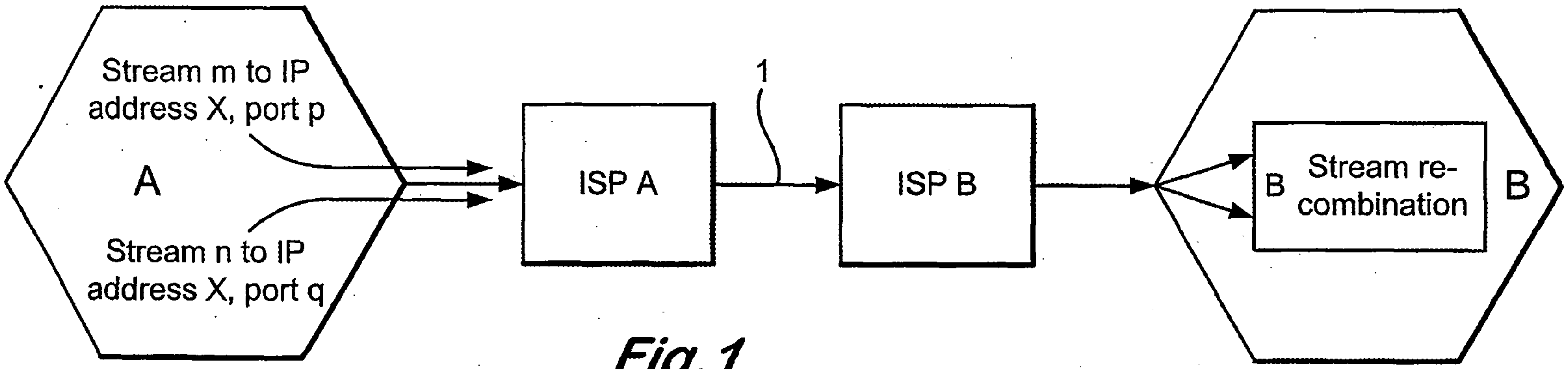

Stream m to IP address X, port p
A
Stream n to IP address X, port q
ISP A
1
ISP B
B
Stream re-combination
B

Fig. 1

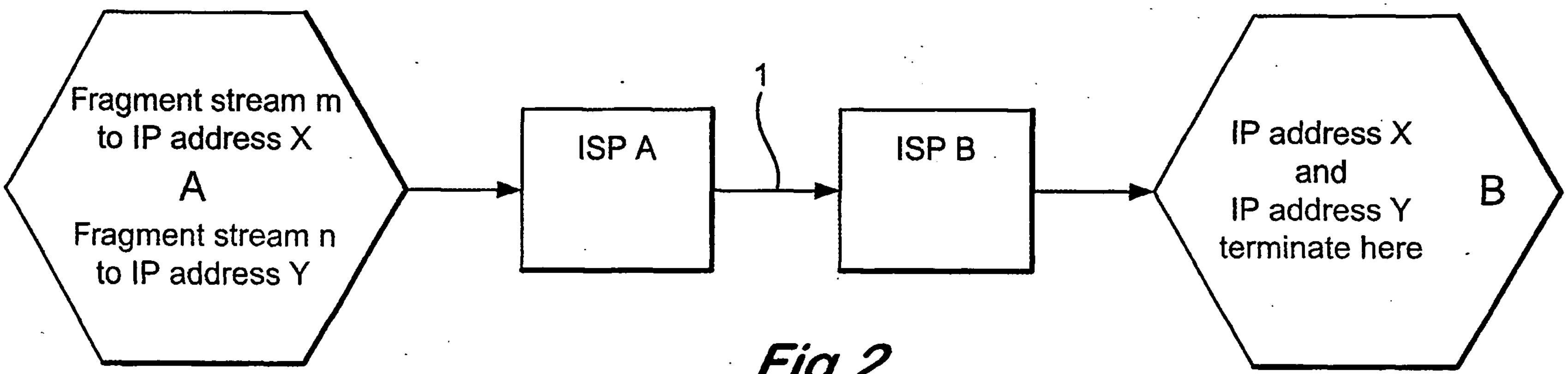

Fragment stream m to IP address X
A
Fragment stream n to IP address Y
ISP A
1
ISP B
IP address X and IP address Y terminate here
B

Fig. 2

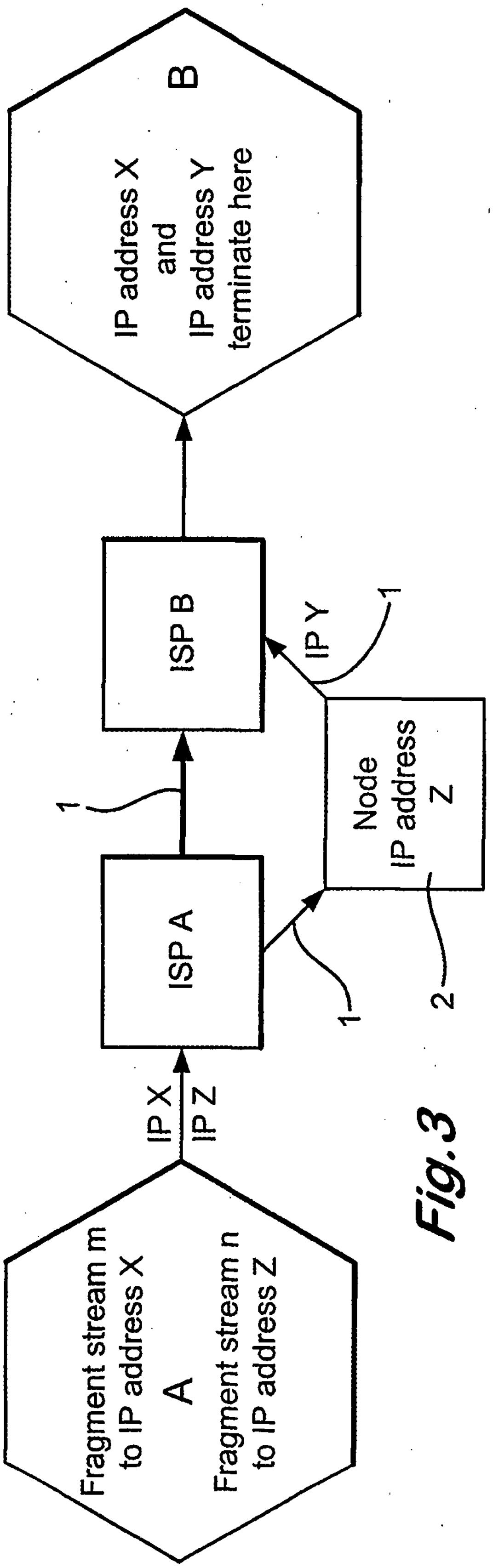

Fragment stream m
to IP address X
A
Fragment stream n
to IP address Z
IP X
IP Z
ISP A
1
1
ISP B
Node
IP address
Z
2
IP Y
1
IP address X
and
IP address Y
terminate here
B

Fig.3

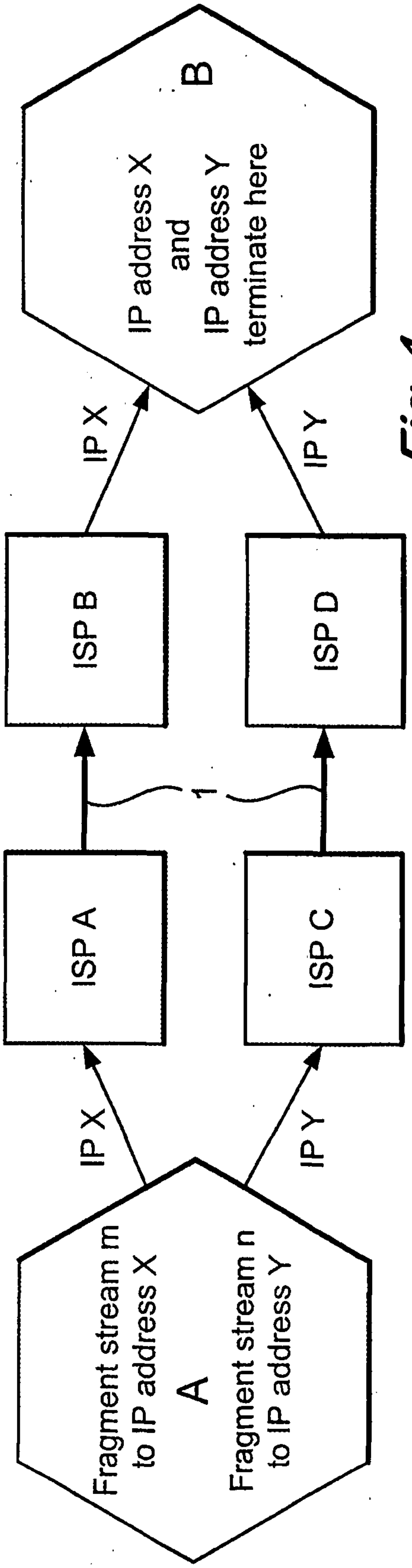

Fragment stream m
to IP address X
A
Fragment stream n
to IP address Y
IP X
IP Y
ISP A
ISP C
1
ISP B
ISP D
IP X
IP Y
IP address X
and
IP address Y
terminate here
B

Fig.4

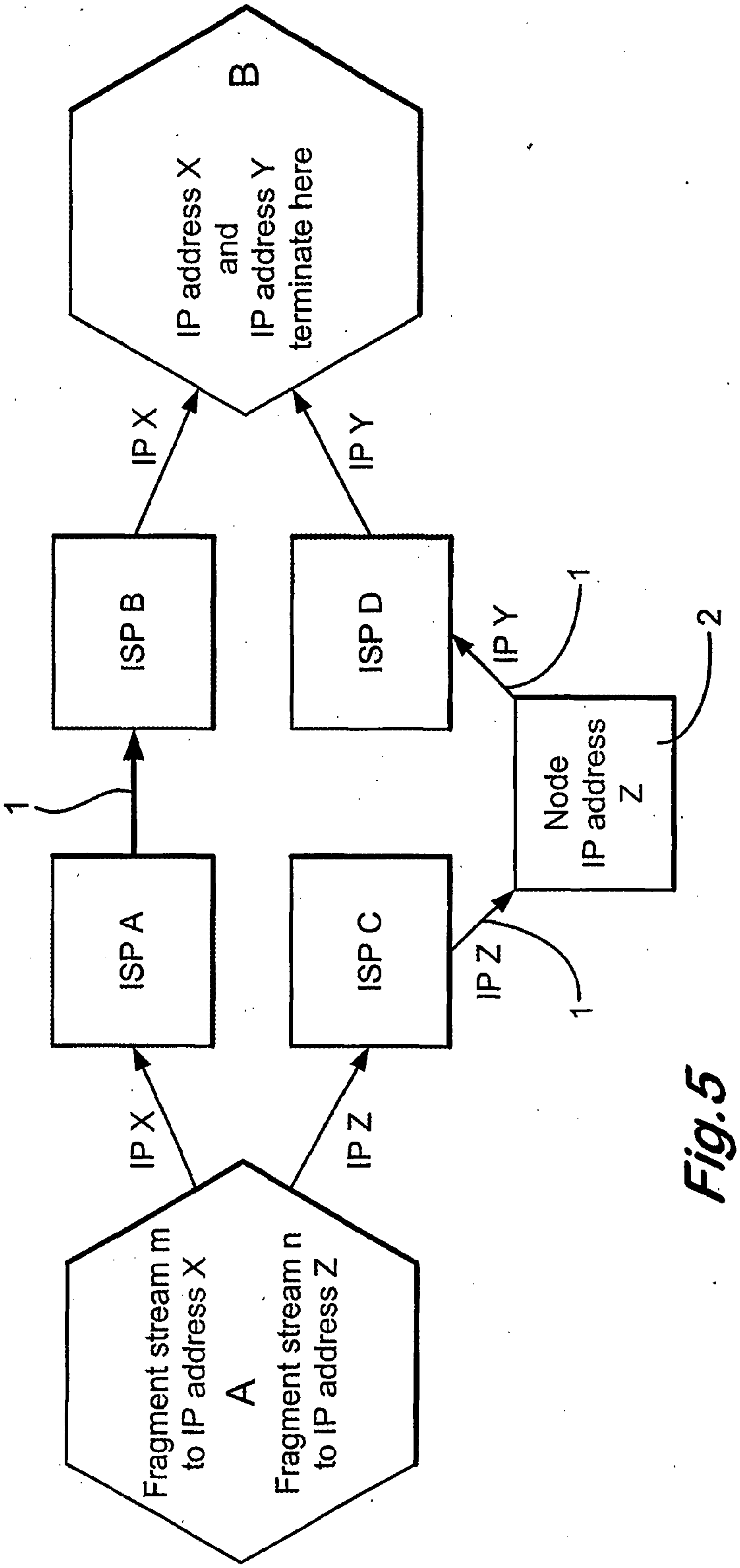

Fragment stream m
to IP address X
A
Fragment stream n
to IP address Z
IP X
IP Z
ISP A
ISP C
1
IP Z
1
Node
IP address
Z
2
ISP B
ISP D
IP Y
1
IP X
IP Y
IP address X
and
IP address Y
terminate here
B

Fig.5

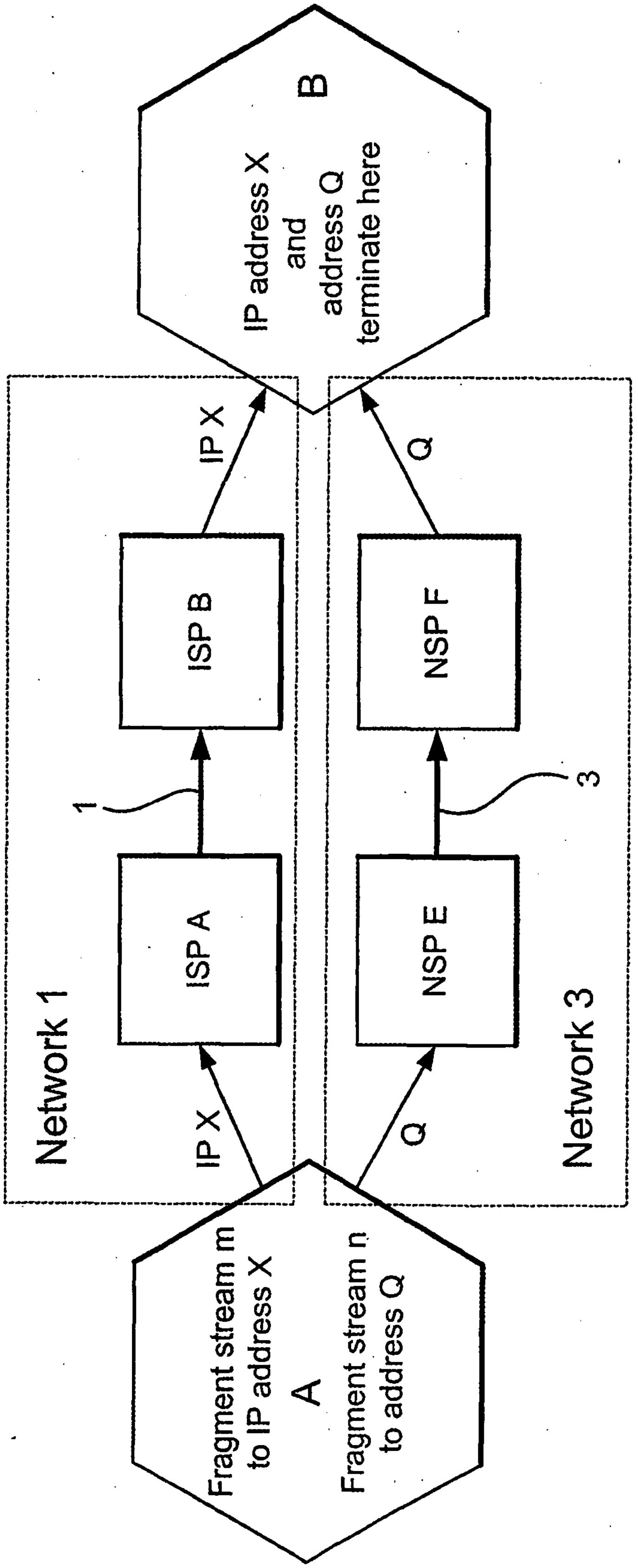

Fragment stream m
to IP address X
A
Fragment stream n
to address Q
IP X
Q
Network 1
Network 3
ISP A
ISP B
NSP E
NSP F
1
3
IP X
Q
IP address X
and
address Q
terminate here
B

Fig.6

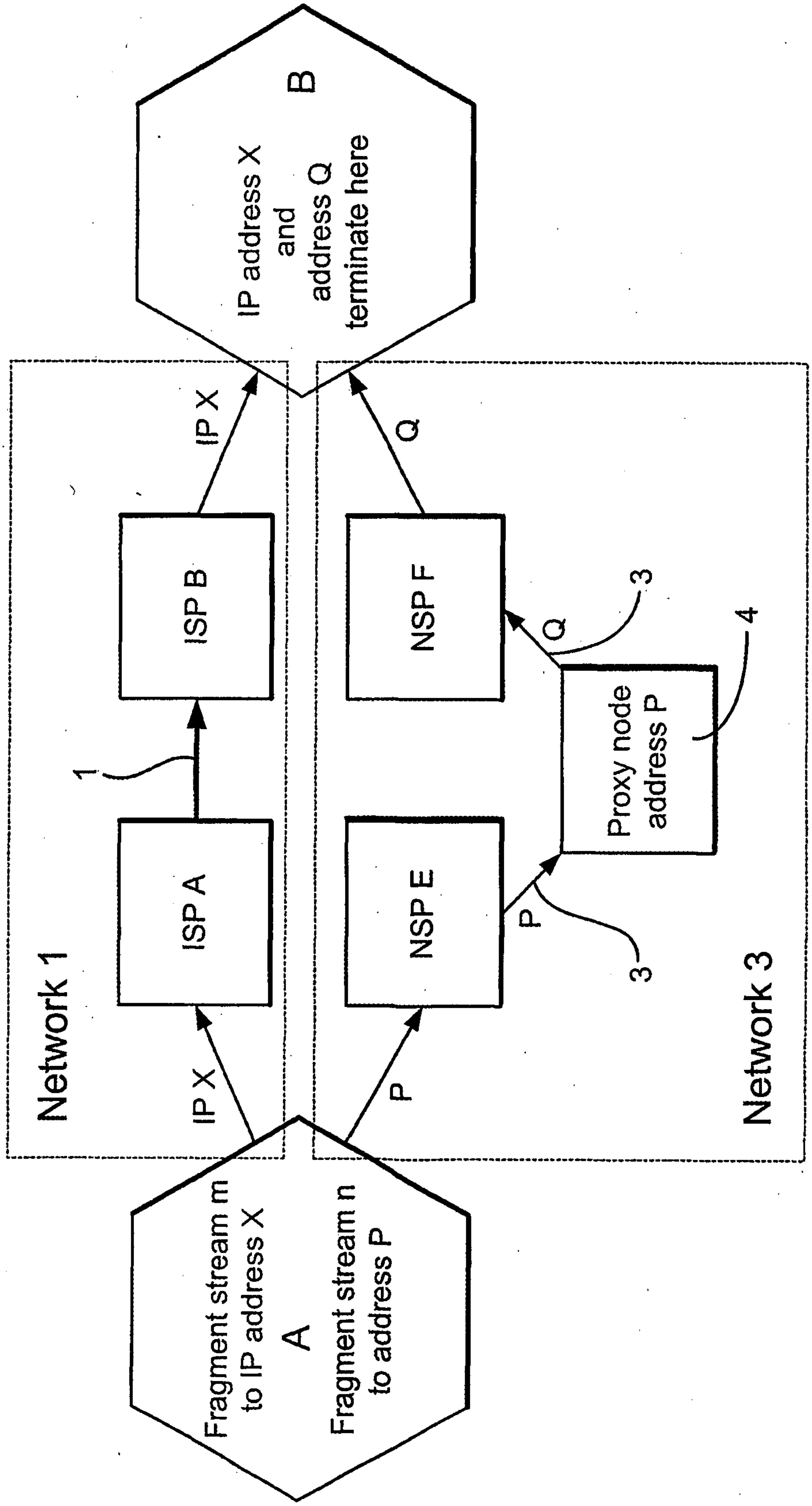

Fragment stream m to IP address X
A
Fragment stream n to address P
Network 1
IP X
ISP A
1
ISP B
IP X
Network 3
P
NSP E
P
3
Proxy node address P
4
Q
3
NSP F
Q
IP address X and address Q terminate here
B

Fig.7

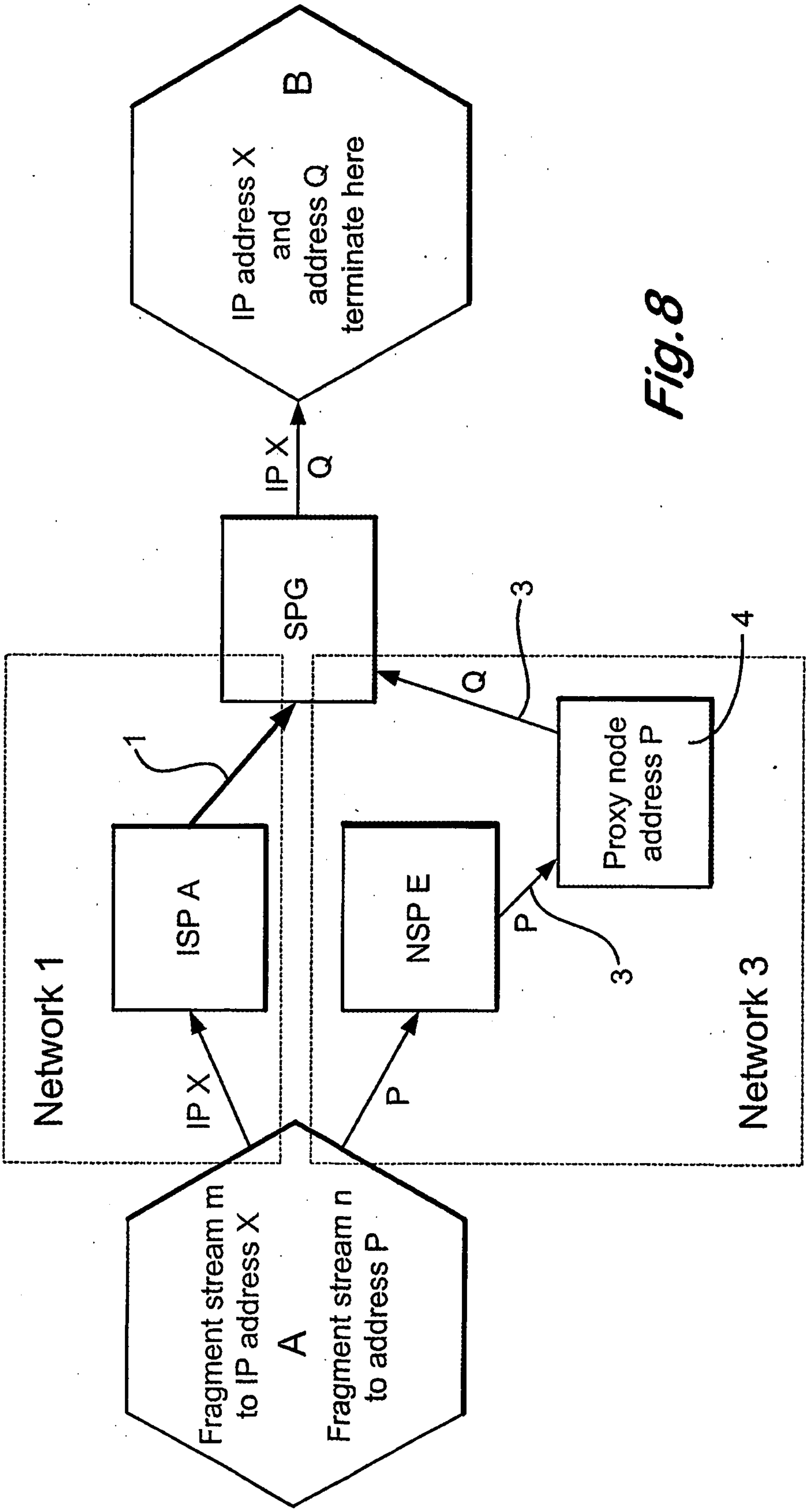

Fragment stream m to IP address X
A
Fragment stream n to address P
Network 1
IP X
ISP A
1
P
NSP E
P
3
Proxy node address P
4
Q
3
Network 3
SPG
IP X
Q
IP address X and address Q terminate here
B

Fig.8

INTERNATIONAL SEARCH REPORT

Intern Application No
PCT/GB 00/04952

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 948 176 A (SIEMENS INF & COMM NETWORKS) 6 October 1999 (1999-10-06) abstract column 1, line 40 -column 2, line 5 figure 1B column 6, line 3 - line 57 column 7, line 18 -column 8, line 45 ---	1,5,6,8, 12
X	WO 00 27086 A (SCHMIDT DOUGLAS CHARLES ;SCIENCE APPLIC INT CORP (US); SHORT ROBER) 11 May 2000 (2000-05-11) abstract page 4, line 10 -page 9, line 13 --- -/--	1-4,7-12

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 3 April 2001	Date of mailing of the international search report 10/04/2001
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Authorized officer Carnerero Álvaro, F

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/GB 00/04952

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	GOGATE N ET AL: "SUPPORTING APPLICATIONS IN A MOBILE MULTIHOP RADIO ENVIRONMENT USING ROUTE DIVERSITY - PART I: NON-REAL TIME DATA" ATLANTA, GA, JUNE 7 - 11, 1998,NEW YORK, NY: IEEE,US, vol. CONF. 5, 7 June 1998 (1998-06-07), pages 802-806, XP000890983 ISBN: 0-7803-4789-7 abstract page 803, right-hand column, paragraph 3 -page 804, left-hand column, paragraph 1	1,12
X	WO 00 18078 A (SOPUCH DAVID J) 30 March 2000 (2000-03-30) abstract page 10, line 25 -page 13, line 18 page 14, line 1 -page 16, line 10	1,7,8,12
A	GB 2 332 833 A (INTERACTIVE MAGAZINES LIMITED) 30 June 1999 (1999-06-30) abstract	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern \pplication No
PCT/GB 00/04952

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0948176 A	06-10-1999	US 6122743 A	19-09-2000
WO 0027086 A	11-05-2000	AU 1455300 A	22-05-2000
		AU 1600300 A	22-05-2000
		WO 0027090 A	11-05-2000
WO 0018078 A	30-03-2000	NONE	
GB 2332833 A	30-06-1999	AU 1775099 A	19-07-1999
		WO 9934547 A	08-07-1999